Frank Field
Education Trust

Social Media Policy and Procedure

Policy Information:

Date prepared	September 2023
Adopted by Board	September 2023
Implementation Date	Immediate
Frequency of Review	Annually
Review Date	September 2024

Approved by CEO: Tom Quinn

Approved by Chair of Board: Dr. Chris Hampshire

Frank Field
Education Trust

1. INTRODUCTION

The internet provides opportunities to participate in interactive discussions and the sharing of information using a wide variety of social media such as Facebook, Twitter, blogs and wikis. However, employees' use of the social media can pose risk to the Trust's confidential proprietary information, reputation and can jeopardise the Trust's legal obligations. The principles set out in this policy are therefore designed to ensure that staff members use social media responsibility so that the confidentiality of pupils and staff and the reputation of the Trust are safeguarded.

2. SCOPE AND PURPOSE

The Frank Field Education Trust (FFET) is committed to making the best use of all available technology and innovation to improve the communication to our stakeholders, children, parents and carers. Technology will enable the Trust to use all reasonable and cost-effective means to improve the way in which we communicate and interact with the communities we serve.

'Social Media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interest online. As the name implies, social media involves building of online communities or networks to encourage participation and engagement.

Social Media platforms open up many opportunities, however the practical application of this technology by the Frank Field Education Trust is continually developing and there may be potential issues to consider both as individual employees and as a Trust. The Trust's IT and Marketing and Communication Manager will provide advice where appropriate.

In order to avoid any mistakes which could result in reputational, legal and ethical issues, and misuse/abuse of an effective social media relationship it is imperative that the Trust IT and Marketing and Communication Manager manages any potential risks by reactively and proactively monitoring social media applications.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the Trust's equipment or facilities are used for the purpose of committing the breach. Staff may be required to remove internet postings which are deemed by the Trust to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

3. WHO IS RESPONSIBLE FOR THE POLICY

The Trust delegate their authority in the manner set out in this policy.

The policy does not form part of any employee's contract of employment and may be amended at any time. The Trust may also vary the procedures set out in this policy including any time limits, as appropriate in any case.

All members of the Trust Executive Team and Academy Senior Leadership Team have responsibility for operating within the boundaries of the policy, ensuring all staff are aware of the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

Training will, if required be provided to facilitate this. All staff are responsible for the success of the policy and should take time to read and understand it. Any misuse of social media should be reported to the CEO or CFOO.

Any questions arising from this policy should be directed to the CFOO or Trust HR Manager.

4. WHO IS COVERED BY THE POLICY

The policy applies to all employees employed on a contract, including the CEO and Senior members of staff.

5. DEFINITION

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or share data in a public forum. This includes email, online social forums, blogs, video and image sharing websites and similar facilities.

Employees should be aware that there are many examples of social media that can be listed separately within this document as this is a constantly changing area. Therefore, employees should follow this policy in relation to any social media that they may use.

6. GENERAL PRINCIPLES

Where the Trust encourages employees to make reasonable and appropriate use of social media websites as part of their work, it is recognised that it is an important part of how the Trust communicates with its audience and allows communication and networking between staff and partners. Employees who have this remit will be advised by their Line Manager /Marketing and Communication Manager.

Employees may with appropriate permission contribute to the Trust's social media activities, for example by writing blogs, managing a social media account and operating an official social communications account for the Trust in accordance with the standards defined by the Principal and or Marketing and Communication Manager.

The Trust understands that employees may wish to use their own computers or devices, such as laptops, tablets and mobile telephones to access social media websites whilst at work, however such access must be in accordance with agreed Acceptable Use Policy.

Employees must be aware that at all times that, while contributing to the Trust's social media activities, they are representing the Trust. Therefore, staff who use social media as part of their job must adhere to the following safeguards: -

- Make sure that the communication has the appropriate purpose and a benefit to the Trust.
- Make sure permission is obtained from a line manager/Marketing and Communication Manager before embarking on a public campaign using social media.
- Ensure a colleague checks the content of any communication before it is published.

Any communication that an employee makes in a professional capacity through social media must not: -

I. Breach confidentiality, for example by:

- Revealing confidential intellectual property or information owned by the Trust or;
- Giving away confidential information about an individual (such as a colleague or partner) or organisation or;
- Discussing the Trust's internal workings (such as agreements that are being reached with a partner/institution or its future business plans that have not been communicated to the public or;
- Doing anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age or;
    - Using social media to bully another individual (such as an employee of the Trust) or:

II. Bring the Trust into disrepute, for example by:

- Criticising or arguing with pupils, customers, colleagues, partners or competitors or:
- Making defamatory comments about individuals or other organisations or groups or:
- Posting images that are inappropriate or links to inappropriate content, or;
- Using somebody else's images or written content without permission; or; Failing to give acknowledgement where permission has been given to reproduce something

7. USE OF SOCIAL MEDIA AT WORK

Employees will be allowed to make reasonable and appropriate use of social media websites from their work devices, provided that any access does not interfere with their duties and is in their own time.

Privacy settings can change without warning, therefore employees are responsible for and should regularly check their privacy settings on networking profiles in order to ensure that they remain secure.

Employees should also be conscious of any posts made that may contravene data protection, privacy, defamation or bullying and harassment.

Employees must not engage in activities involving social media that are capable of bringing the Trust into disrepute.

Staff must not use social media or the internet in any way to attack, insult, abuse or defame pupils, their family members, and colleagues, other professionals, third parties, organisations or the Trust.

Employees must not represent personal opinions as those of the Trust on any social medium and employees acting in a professional capacity using the reputation and name of the Trust for blogs, tweets, articles and social media communication must have Trust permission to do so.

Trust email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media. Employees must not edit open access online encyclopaedia's such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it is the Trust.

8. MONITORING OF SOCIAL MEDIA DURING WORK

The Trust reserves the right to monitor employees' internet usage in accordance with the Information Acceptable Use Policy and the Data Protection Act 2018.

It is expected that employees will not spend an excessive amount of time using social media websites for non-work related activity; or act in a way that is in breach of the rules set out in this policy.

The IT department have the right to withdraw access to particular social media websites in the case of any misuse or inappropriate links or articles, once agreed with the CEO or CFOO.

9. SOCIAL MEDIA FOR PERSONAL LIFE

The Trust recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the Trust, employees must be aware that they can damage the Trust if they are recognised as being an employee of the Trust and the posting of messages or material is offensive or inappropriate.

Employees are allowed to say that they work for the Trust, which recognises that it is natural for its staff to sometimes discuss their work and profession on social media. However the employee's online profile should not be focused to the area in which the employee works (e.g. specific Academy)

If an employee does discuss work on social media (for example giving opinions on their specialism or the sector in which the Trust operates) they are advised to include a profile statement which will state "The views I express here are mine alone and do not necessarily reflect the views of my employer".

Any communications that an employee makes in a **personal capacity** through social media must not:-

Breach confidentiality, for example by:-

- Revealing confidential intellectual property or information owned by the Trust or;
- Giving away confidential information about an individual (such as a colleague or partner contact) or organisation / partner institution or;
- Discussing the Trust's internal workings (e.g. agreements that it is reaching with partner institutions/customers or its future business plans that have not been officially communicated to the public) or ;
- Do anything that could be considered discriminatory against, or bullying or harassment of any individual, for example by:
    - Making offensive or derogatory comments
    - Using social media to bully another individual or;
- Posting images that are discriminatory or offensive or links to such content or;
- Bring the Trust into disrepute, for example by;
    - Criticising or arguing with colleagues, customers, partners or competitors or;
    - Posting images that are inappropriate or links to inappropriate content or;

Breach copyright, for example by:

- Using someone else's images or written content without permission; or
- Failing to give acknowledgement where permission has been given to reproduce something.

10. SOCIAL MEDIA AND SAFEGUARDING

Employees are reminded that they should not engage **in any online activity** that may compromise or question their professional conduct and responsibilities.

If a current or ex pupil (other than relatives or close family friend) requests interaction through personal (non-Trust official) social media account e.g. Flickr, Bebo, Facebook, Instagram etc. of an employee, the employee is reminded that such interaction **is not permitted** and may compromise their professional conduct and responsibilities.

Employees must not have contact through any social medium with any pupil of the Trust unless the pupils are family members.

Employees must decline 'friend requests' from pupils and ex pupils (other than relatives or close family friends) that they receive through personal social media accounts. On leaving the Trust, employees must not contact the Trust's pupils by means of personal social media sites. Similarly, employees must not contact pupils from their former schools by means of personal social media.

Employees should be aware that their reputation may be harmed by what others share about them online. E.g. friends or associates tagging in an inappropriate post, photograph or video, which may breach code of conduct or professional standards.

If an employee sees or is aware of content in social media that disparages or reflects poorly on the Trust or any employee it should be reported to the CEO. Employees should not attempt to rectify an issue alone.

11. SOCIAL MEDIA AND DISCIPLINARY ACTION

Employees are required to adhere to this policy and guidelines. All employees should be aware that use of social media in a way that may be deemed as deliberate or inadvertent misuse which could breach this policy and guidelines may constitute misconduct and may lead to action under the Trust's Disciplinary procedure up to and including dismissal.

12. PUBLIC INTEREST DISCLOSURE ('WHISTLE BLOWING')

Where an employee releases information through Social Media that may be considered as a Public Interest Disclosure ('Whistle Blowing'), the Trust 'Whistle Blowing' procedure must be initiated in the immediate instance before any further action is taken.

13. REVIEW

Due to the changing nature of information technology and particularly social media and electronic communication, this policy and guidelines will be reviewed in line with the agreed review time of every two years. However, should any issue be highlighted by the Information Technology Team or Senior Management in relation to new developments and progression

with Social Media, then the Trust will review this policy and guidelines more regularly and make relevant amendments.

Any proposed changes will be considered by the Trust Board for approval. Any amendments will be communicated to employees and professional associations accordingly.

15 GENERAL PRINCIPLES UNDERLYING THIS POLICY

This policy will operate in accordance with the provisions of the **Data Protection Act 2018**

This policy has been developed in accordance with the **ACAS guidelines on Social Media in the workplace.**

Grievances - Where an employee raises a grievance in relation to social media the Grievance Procedure will be used in conjunction with the Social Media Policy. Advice should be sought from Human Resources.

Discipline – Where it is found that a breach in the Social Media Policy and Procedures is evident then the Trust's Discipline Procedure will be used.

Monitoring and Evaluation - The Trust will monitor the operation and effectiveness of the Social Media Policy and ensure arrangements and legislation remain current.

This policy has been developed in accordance with the statutory guidance of **Keeping children safe in education.**